Лекция 3
Теорема Лагранжа

Определение. Пусть $(G, \star)$ — группа. *Подгруппой* группы G называется подмножество $H \subset G$, которое образует группу относительно той же операции $\star$. Иными словами, подмножество H, претендующее на звание подгруппы, должно обладать двумя свойствами:

1°. (замкнутость относительно умножения) Если $h_1, h_2 \in H$, то $h_1 \star h_2 \in H$.

2°. (замкнутость относительно перехода к обратному) Если $h \in H$, то $h^{-1} \in H$.

(Остальные два свойства. входящие в определение группы: ассоциативность и наличие нейтрального элемента — выполняются в данном случае автоматически.)

Замечание. Если группа G конечна, то для подмножества $H \subset G$ свойство 2 вытекает из свойства 1.

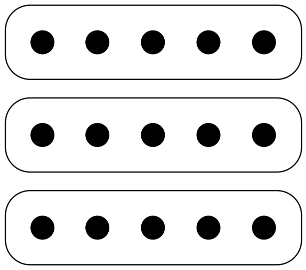
Примеры.

1. В любой группе есть две *несобственные* подгруппы: тривиальная (состоящая из одного единичного элемента) и полная (вся группа).
2. Рассмотрим аддитивные числовые группы $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$. Тогда в цепочке $\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R}$ каждая группа является подгруппой следующей.
3. Для любого n имеем: $C_n \subset D_n$ — подгруппа.
4. Перечислим все подгруппы группы D_3, глядя на ее таблицу умножения и рассуждая, исходя непосредственно из определения подгруппы. Получим, что, помимо двух несобственных подгрупп, имеются еще три подгруппы порядка 2 (каждая из них включает тождественное преобразование и одно из отражений) и одна подгруппа порядка 3, состоящая из трех вращений, включая тождественное.

Заметим, что во всех приведенных примерах наблюдается такое явление: если группа конечна и имеет порядок n, то подгруппы у нее бывают только таких порядков m, которые являются делителями числа n. Например, в группе D_3, имеющей порядок 6, нет ни одной подгруппы порядка 4. Это не случайно. На самом деле имеет место такая общая теорема.

Теорема Лагранжа. Порядок конечной группы делится нацело на порядок любой ее подгруппы.

Доказательство. Оказывается, что множество всех элементов группы G можно разбить на несколько непересекающихся подмножеств, каждое из которых содержит ровно столько элементов, сколько подгруппа H. Эта конструкция называется *разбиением группы на смежные классы по подгруппе*, и из нее очевидным образом вытекает утверждение теоремы.



Смежные классы в группе порядка 15 по подгруппе порядка 5

Разбиение группы на смежные классы строится следующим образом. Пусть $H = \{h_1, ..., h_m\}$. Для произвольного элемента $g \in G$ положим

$$gH = \{gh_1, ..., gh_m\}.$$

Множество gH называется смежным классом. В нем, очевидно, столько же элементов (m), сколько в подгруппе H. Заметим, что для разных элементов g_1 и g_2 смежные классы g_1H и g_2H могут, вообще говоря, совпадать (т.е. списки $\{g_1h_1, ..., g_1h_m\}$ и $\{g_2h_1, ..., g_2h_m\}$ могут отличаться только порядком перечисления). Это так, например, если g_1 и g_2 оба принадлежат подгруппе H — в этом случае $g_1H = g_2H = H$.

Но — что очень важно — смежные классы g_1H и g_2H не могут совпадать частично, т.е. если у них хотя бы один общий элемент, то они совпадают целиком. Для доказательства этого факта предположим, например, что $g_1h_1 = g_2h_2$. Отсюда вытекает, что элементы g_1 и g_2 отличаются друг от друга умножением на какой-то элемент подгруппы H: $g_1 = g_2h_2h_1^{-1}$, $g_2 = g_1h_1h_2^{-1}$. Следовательно, любой элемент смежного класса g_1H можно записать так:

$$g_1h = g_2(h_2h_1^{-1}h) \in g_2H,$$

поскольку $h_2h_1^{-1}h \in H$. Точно так же получается, что любой элемент из множества g_2H принадлежит множеству g_1H. Следовательно, $g_1H = g_2H$, что и требовалось. Доказательство окончено.

Задача на дом. Перечислить все подгруппы в группах C_6, D_2.